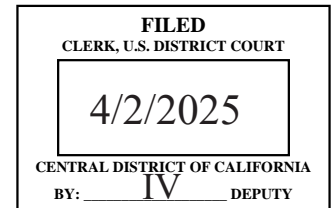


UNITED STATES DISTRICT COURT

for the

Central District of California



United States of America

v.

Jose Henry Ayala Casimiro,
 aka "Henry Ayala,"
 aka "ayalahenry818,"
 aka "Cocohennn,"
 aka "CocohennnnXdddd,"

Defendant.

Case No. 2:25-MJ-01947-DUTY

**CRIMINAL COMPLAINT BY TELEPHONE
 OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning on or before July 25, 2022, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section

18 U.S.C. § 2252A(a)(5)(B)

Offense Description

Possession of Child Pornography

This criminal complaint is based on these facts: *Please see attached affidavit.*

☒ Continued on the attached sheet.

/s/ Carolyn Thompson

Complainant's signature

Carolyn Thompson, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: April 2, 2025

Judge's signature

City and state: Los Angeles, California

Hon. Patricia Donahue, U.S. Magistrate Judge

Printed name and title

AUSAs: David Ryan 213-894-4491
 Amanda Elbogen 213-894-5647

AFFIDAVIT

I, Carolyn Thompson, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrant against Jose Henry Ayala Casamiro ("AYALA") for a violation of Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography and attempted possession of child pornography).

2. This affidavit is also made in support of applications for warrants to search the premises located at 11150 Glenoaks Blvd. Unit 61 (the "SUBJECT PREMISES"), as further described in Attachment A-1; and the person of Jose Henry Ayala Casimiro ("AYALA," or the "SUBJECT PERSON"), as further described in Attachment A-2.

3. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 2251(a) (sexual exploitation of children and attempted sexual exploitation of children); Title 18, United States Code, Section 2252A(a)(2) (distribution and receipt of child pornography and attempted distribution and receipt of child pornography); and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography and attempted possession of child pornography) (collectively, the "Subject Offenses"), as described more fully in Attachment B. Attachments A-1, A-2, and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrants, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates and times are on or about those indicated.

II. BACKGROUND OF AFFIANT

5. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed as such since July 2024. I am currently assigned to a Joint Terrorism Task Force Squad at the West Covina Resident Agency of the Los Angeles Field Office. During my career, I have participated in multiple criminal and national security investigations, to include those involving the use of digital devices and online accounts to facilitate violations of federal law. Through the course of my training and employment with the FBI, I have used a variety of investigative techniques and resources, including the execution of search warrants and review of both physical and digital evidence collected from search warrant returns. I am familiar with the strategy, tactics, methods, tradecraft, and techniques of criminals, terrorists, and their agents. During my employment with the FBI, I attended New Agent Training at the

FBI Academy in Quantico, Virginia from July to December 2024. I have received additional formal and informal training from the FBI regarding criminal and counterterrorism investigations, to include training concerning the use of electronic communications and digital devices in furtherance of a crime. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

III. SUMMARY OF PROBABLE CAUSE

6. In August 2023, AYALA possessed Child Sexual Abuse Material ("CSAM") on his social media and email accounts. The CSAM includes videos in which AYALA can be seen and heard directing minors to engage in sexually explicit behavior.

7. AYALA caused minors to produce CSAM as well as other video content depicting themselves engaging in self harm as part of his participation in an online network known as "764", a network of nihilistic violent extremists who engage in criminal conduct, particularly targeting children for sexual exploitation online, to further the network's goals of accelerating social unrest and the downfall of the current world order, including the United States Government.

8. Information provided by a minor victim in February 2025 and records provided by a social media company in March 2025 indicate that AYALA continues to interact with minors online, including in an online forum designed as a "grooming pool" for underage girls.

9. Subscriber information from AYALA's online accounts, law enforcement databases, and surveillance conducted by FBI agents, all indicate that he resides at the SUBJECT PREMISES.

IV. STATEMENT OF PROBABLE CAUSE

10. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. July 2022-August 2023: AYALA Possessed and Produced Child Sexual Abuse Material Online

1. Background on the National Center for Missing and Exploited Children ("NCMEC")

11. NCMEC functions as a national clearinghouse for information on missing and exploited children and the sexual exploitation of children. Electronic Service Providers ("ESPs") and members of the public can report suspected child exploitation to NCMEC through its CyberTipline. ESPs include companies such as Discord and Meta Platforms, which provide free and paid services online. These services may include email, instant messaging, social networking, and online file transfer or storage. NCMEC provides information to law enforcement agencies through CyberTipline Reports.

12. ESPs may discover suspected child exploitation files through user reports, automated scanning of a hash value¹

¹ A "hash value" is a numerical identifier for digital data, such as a particular file. It is obtained by using a mathematical function, often called an algorithm. When a hash value is generated for an image file, any other identical image file will have the same hash value. However, if the data is changed, even very slightly (such as the addition or deletion of a single pixel in an image), the hash value will change. Thus, a hash
(footnote cont'd on next page)

associated with a particular file depicting child pornography, and other methods.

2. July 2022: AYALA Possessed CSAM on His Social Media Account

13. In July 2022, Social Media Company #1 sent CyberTipline Report 129293315 to NCMEC, advising that a specified user account was connected to an incident on or about July 25, 2022, in which suspected CSAM was uploaded, downloaded, sent, or received on Social Media Company #1. The CyberTipline Report provided the following information for the user account at issue: the username was "cocoheennn", and the subscriber information for the user included a date of birth of March 22, 1997, and an email address "ayalahenry818" followed by a domain name belonging to a different company ("Social Media Company #2"). Based on my review of public and law enforcement databases, I know that March 22, 1997, is AYALA's date of birth. The CyberTipline Report also stated that the user account used IP address 142.129.44.180.

14. Based on my conversation with other law enforcement officers who reviewed the video file, it is a 20-second video depicting an apparent minor female, approximately 10-12 years of age, being anally penetrated by the erect penis of an adult male.

value can be thought of as a "digital fingerprint" for data -- if two images have the same hash value, there is an extremely high likelihood that the images are the same.

3. August 2023: AYALA Possessed CSAM on his Email Account

15. In August 2023, the Los Angeles Police Department ("LAPD") obtained search warrants in the Los Angeles County Superior Court for the contents of the "cocoheennn" account with Social Media Company #1 and the "ayalahenry818" account with Social Media Company #2 for evidence related to violations of California Penal Code Section 311.11 (Possession, Manufacture, and Distribution of Child Sexual Abuse Material). That warrant and supporting application are attached as Exhibit 1 and incorporated herein by reference.

16. Social Media Company #1 provided information on the "cocoheennn" account in response to the warrant. The search warrant return identified two videos and the account name. The "cocoheennn" account was deleted on or about July 26, 2022, the same day as the NCMEC report described above.

17. On March 7, 2025, LAPD provided the FBI a flash drive containing the records provided by Social Media Company #2 in response to the August 2023 warrant for the "ayalahenry818" account. On or about March 20, 2025, Social Media Company #2 provided additional information regarding the "ayalahenry818" account. The payment information for the account listed AYALA's full name. The IP address information indicated that AYALA accessed the internet from the SUBJECT PREMISES at least as recently as March 19, 2025.

18. I reviewed California Department of Motor Vehicles database information for AYALA and saw that he is a 28-year-old male, and his residence is listed as the SUBJECT PREMISES.

19. In March 2025, I reviewed the contents of the flash drive provided by LAPD and identified the following:

a. The records included over 50 images and videos of that appear to depict the production and attempted production of CSAM. In addition, there were over 100 images and videos of child erotica. Four sample videos are described as follows:

i. Video 1, titled "Record_2022-12-11-04-01-57-1lmh2fxb82f8i.mp4" is 56 seconds in length. The video is a screen recording of a video call between AYALA and an approximately 14-year-old minor female ("MINOR VICTIM 1"). As described further below, after the production of Video 1, law enforcement identified and interviewed MINOR VICTIM 1. According to public databases, MINOR VICTIM 1 was born in 2008. In Video 1, MINOR VICTIM 1 is depicted naked and laying down on her back perpendicular to the camera with her face and feet out of view. In the video, AYALA's face appears on the screen, which I can recognize based on comparing his face to his California DMV photograph. In the video, AYALA uses the first name of MINOR VICTIM 1, stating, "yeah, keep going." MINOR VICTIM 1 refers to AYALA in the video by his first name, "Henry." In the video, MINOR VICTIM 1 can be seen with her hand between her legs in the vicinity of her vaginal area appearing to masturbate while AYALA can be seen and heard providing her specific directions.

ii. Video 2, titled "2023-05_3113_45-1j04fepts137m.mp4" is 23 seconds in length. The video contains what appears to be a pubescent female approximately 13-14 years old. While the female's face is not visible in Video 2, based on my review of Video 2 as well as additional images and videos containing imagery of MINOR VICTIM 1's bedroom and clothing, as well as conversations with other law enforcement, I believe the person in the video is likely MINOR VICTIM 1. In the video, the female is laying on a bed with her face and feet obscured with her vaginal region displayed for the camera. During the video, the female can be seen using what appears to be the handle of a hairbrush to vaginally penetrate and masturbate in display of the camera.

iii. Video 3, titled "Screen_Recording_20230609_1-1j14wqbl5v2xe.mp4" is 16 minutes and 56 seconds in length. The video is a screen recording of a video conversation between AYALA and a pubescent female who appears to be approximately 13-15 years old. In the beginning of the video, AYALA's face appears in the screen capture and when his face is not displayed, his camera icon shows the letter "H". Furthermore, during the recording, the female refers to AYALA by his name, stating, "Henry, if I see you again we gon' fight". In the video, the female is naked with her vaginal region and breasts displayed for the camera. The female masturbates while holding one of her breasts. At the end of the video, the female asks AYALA to tell her when he is finished.

iv. Video 4, titled "22-06-01-19-10-17-1imgxznate8o2.mp4" is 9 minutes and 21 seconds in length. The video is a screen recording of a video chat between AYALA and a pubescent female who appears to be approximately 14-16 years old. Based on review of additional videos where AYALA speaks and can also be identified by his face, I know the voice in the video belongs to AYALA. In the video, the female is in a room naked. During the video, the female shows her anal and vaginal regions to the camera and masturbates in a chair while communicating with AYALA, whose voice can be heard in the background. At the end of the video, AYALA stated that he had ejaculated while watching the female.

B. AYALA Caused Minors to Create CSAM in Connection with His Participation in the "764" Network

1. Background on Nihilistic Violent Extremism ("NVE") and the "764" Network

20. Based on my training and experience and discussions with other FBI special agents, I understand the following about NVE and "764":

a. Nihilistic Violent Extremists ("NVE"s) are individuals who engage in criminal conduct within the United States and abroad, in furtherance of political, social, or religious goals that derive primarily from a hatred of society at large and a desire to bring about its collapse by sowing indiscriminate chaos, destruction, and social instability. NVEs work individually or as part of a network with these goals of destroying civilized society through the corruption and

exploitation of vulnerable populations, which often include minors.

b. NVEs, both individually and as a network, systematically and methodically target vulnerable populations across the United States and the globe. NVEs frequently use social media communication platforms to connect with individuals and desensitize them to violence by, among other things, breaking down societal norms regarding engaging in violence, normalizing the possession, production, and sharing of CSAM and gore material, and otherwise corrupting and grooming those individuals towards committing future acts of violence.

c. Those individuals are targeted online, often through synchronized group chats. NVEs frequently conduct coordinated extortions of individuals by blackmailing them so they comply with the demands of the network. These demands vary and include, but are not limited to, self-mutilation, online and in-person sexual acts, harm to animals, sexual exploitation of siblings and others, acts of violence, threats of violence, suicide, and murder.

d. Historically, NVEs systematically targeted vulnerable individuals by grooming, extorting, coercing, and otherwise compelling through force, or the threat of force, the victims to mutilate themselves or do violence, or threaten violence, to others, and either film or photograph such activity. The members of the network have edited compilation photographs or videos of targeted individuals and shared the photographs and videos on social media platforms for several

reasons, including to gain notoriety amongst members of the network, and spread fear among those targeted individuals for the purpose of accelerating the downfall of society and otherwise achieving the goals of the NVEs.

e. NVEs have adopted various monikers to identify themselves. The networks have changed names over time, which has led to the creation of related networks. Although the networks change names and use a variety of different social media platforms, the core members and goals remain consistent and align with the overarching threat of NVE.

f. "764" and related groups are NVEs who engage in criminal conduct within the United States and engage with other extremists abroad. The 764 network's accelerationist goals include social unrest and the downfall of the current world order, including the United States Government. Members of 764 work in concert with one another towards a common purpose of destroying civilized society through the corruption and exploitation of vulnerable populations, including minors.

2. AYALA Caused Minors to Produce CSAM and Videos of Themselves Engaging in Self-Harm in Furtherance of His Participation in the 764 Network

21. Records provided by Social Media Company #2 in response to the August 2023 warrant included a photograph from March 2020, in which an individual had cut the name "Henry" into their right forearm.

22. In 2022 and 2023, NCMEC received multiple CyberTipline reports that specifically identified AYALA by name, as well as other individuals, as being involved in the creation,

possession, and distribution of CSAM. The tips described how AYALA and other identified males would "blackmail underage girls into getting nude and writing names on their skin, cutting, and sticking objects into genitals such as knives (*sic*) and bottles." For example, in June 2023, CyberTipline report 163900925 stated that an individual "reported [AYALA] got the child to put a H on her body (a self carving). Other children have done the same for the reported person." This CyberTipline report stated that the tipster was the sister of MINOR VICTIM 1. Also in June 2023, MINOR VICTIM 1 herself submitted multiple CyberTipline reports to NCMEC in which MINOR VICTIM 1 described having an online relationship with AYALA. In the report, MINOR VICTIM 1 identified the SUBJECT PREMISES as AYALA's home address.

23. I reviewed a Homeland Security Investigations report of an interview of MINOR VICTIM 1 conducted in April 2023. MINOR VICTIM 1 stated that AYALA made MINOR VICTIM 1 do sexual things on camera such as touch herself. MINOR VICTIM 1 stated that AYALA made girls he met online do things like throw up on camera and then lick it up. MINOR VICTIM 1 also reported that AYALA made girls put cigarette butts out on their skin and cut themselves.

24. In May 2023, NCMEC received an anonymous CyberTipline report (165188040) regarding a group known as "H3ll" on a social media platform ("Social Media Company #3) that included "degrading sadistic sexual acts, torture sessions, 'Cutting or

Carving Sessions' (CVLT),² and encouraging young females to commit suicide" An account on Social Media Company #3 with username "CocohennnnXdddd" was listed as a member of this H3ll group. This username, similar to AYALA's "Cocohennn" username with Social Media Company #1, was reported to NCMEC by MINOR VICTIM 1 as belonging to AYALA in CyberTipLine report number 164322023.

C. February – March 2025: AYALA Continues to Interact with Minors Online

25. On or about February 15, 2025, the FBI's Internet Crime Complaint Center received a tip, later forwarded to NCMEC, stating that a 17-year-old who was a groomed member of CVLT created a new server on a social media application for AYALA, whom the tipster identified by name, and other individuals. The tipster indicated the server acted as a "grooming pool" with many underage girls exposed to and "predated upon."

26. In March 2025, Social Media Company #2 provided information regarding the "ayalahenry818" email account. Based on my review of those records, on March 13, 2025, from approximately 12:00 A.M. to 2:00 A.M. and again from approximately 11:15 A.M. to 1:03 P.M., AYALA engaged in a group chat organized by an individual using an email address with a domain name that belongs to a public school district in Colorado. FBI Agents asked officials from the school district

² Based on my training and experience, I know that "CVLT" is an NVE network that is similar to and predates the "764" network.

to identify the user, who subsequently identified the user as a minor student in that school district ("COLORADO MINOR 1").

27. Records from Social Media Company #2 also show that on March 14, 2025, from 9:31 A.M. to 10:27 A.M., AYALA engaged in an online chat with an individual using a different email with a domain belonging to the same public school district in Colorado. Officials from the school district identified the user as another minor student from the district ("COLORADO MINOR 2").

D. AYALA Resides at the SUBJECT PREMISES

28. According to the California Department of Motor Vehicles ("DMV"), AYALA's current residence is listed as the SUBJECT PREMISES.

29. According to IP address information provided by Charter Communications, the IP address AYALA utilized to access the "ayalahenry818" account during the timeframe of the online chats with COLORADO MINOR #1 and COLORADO MINOR #2 in March 2025 was subscribed to by AYALA's mother at the SUBJECT PREMISES.

30. Based on information provided by Social Media Company #2 on March 20, 2025, the "ayalahenry818" account had been accessed from the SUBJECT PREMISES as recently as 4:18 A.M. on March 19, 2025.

31. On April 1, 2025, FBI Special Agents conducted physical surveillance at the SUBJECT PREMESIS and observed AYALA departing the residence.

V. BACKGROUND ON CHILD EXPLOITATION OFFENSES, COMPUTERS, THE INTERNET, AND DEFINITION OF TERMS

32. In this affidavit, the terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

33. Based upon my training and experience in the investigation of child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers with child pornography:

a. Computers and Child Pornography. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can convert these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. File Storage. Computer users can choose their method of storing files: either on a computer's hard drive, an external hard drive, a memory card, a USB thumb drive, a smart phone or other digital media device, etc. (i.e., "locally") or on virtual servers accessible from any digital device with an Internet connection (i.e., "cloud storage"). Computer users

frequently transfer files from one location to another, such as from a phone to a computer or from cloud storage to an external hard drive. Computer users also often create "backup," or duplicate, copies of their files. In this way, digital child pornography is extremely mobile and such digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto external hard drives small enough to fit onto a keychain. Just as easily, these files can be copied onto compact disks and/or stored on mobile digital devices, such as smart phones and tablets. Furthermore, even if the actual child pornography files are stored on a "cloud," files stored in this manner can only be accessed via a digital device. Therefore, viewing this child pornography would require a computer, smartphone, tablet, or some other digital device that allows the user to access and view files on the Internet.

c. Internet. The term "Internet" is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

d. Internet Service Providers. Individuals and businesses obtain access to the Internet through ISPs. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

e. IP Addresses. An Internet Protocol address ("IP Address") is a unique numeric address used to connect to the Internet. An IPv4 IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). In simple terms, one computer in a home may connect directly to the Internet with an IP Address assigned by an ISP. What is now more typical is that one home may connect to the Internet using multiple digital devices simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems, by way of example. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home are connected to

the Internet via a router or hub. Internet activity from every device attached to the router or hub is utilizing the same external IP Address assigned by the ISP. The router or hub "routes" Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. The IP Address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP Address is only assigned for the duration of that online session. Most ISPs maintain records of which subscriber was assigned which IP Address during an online session.

f. IP Address - IPv6. Due to the limited number of available IPv4 IP addresses, a new protocol was established using the hexadecimal system to increase the number of unique IP addresses. An IPv6 consists of eight sets of combination of four numbers 0-9 and/or letters A through F. An example of an IPv6 IP address is 2001:0db8:0000:0000:0000:ff00:0042:8329.

g. The following definitions:

i. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

ii. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other

individuals. Individuals may also have the ability to transmit links to electronic files to other individuals within the chat room.

iii. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

iv. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where: (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

v. "Cloud-based storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet. Users of such a service can share links and associated passwords to their stored files with other traders of

child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is typically free and readily available to anyone who has an Internet connection.

vi. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

vii. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related

communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

viii. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

ix. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

x. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as

the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

xii. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

xiii. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

xiv. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

xv. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP

addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

xv. "Log files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

xvi. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

xvii. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

xviii. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in

handmade, photographic, mechanical, electrical, electronic, or magnetic form.

xix. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

xx. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

xxi. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

xxii. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

xxiii. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text

Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

VI. TRAINING & EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

34. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media, or from literature describing such activity. These individuals often maintain possession of these items for long periods of time and keep their collections in numerous places - in digital devices in their homes, in their cars, in their workplaces, or on their persons.

b. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials (including through digital distribution via the Internet); conceal such correspondence as they do their sexually explicit material; and

often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. These individuals often maintain possession of these items for long periods of time.

35. Digital child pornography on a digital device is easy to maintain for long periods of time. Modern digital devices often have extremely large storage capacities. Furthermore, cheap and readily available storage devices, such as thumb drives, external hard drives, and compact discs make it simple for individuals with a sexual interest in children to download child pornography from the Internet and save it - simply and securely - so it can be accessed or viewed indefinitely.

36. Furthermore, even if a person deleted any images of child pornography that may have been possessed or distributed, there is still probable cause to believe that there will be evidence of the illegal activities - that is, the possession, receipt, and/or distribution of child pornography - at the SUBJECT PREMISES or on his person. Based on my training and experience, as well as my conversations with digital forensic experts, I know that remnants of such files can be recovered months or years after they have been deleted from a computer device. Evidence that child pornography files were downloaded and viewed can also be recovered, even after the files themselves have been deleted, using forensic tools. Because remnants of the possession, distribution, and viewing of child pornography is recoverable after long periods of time, searching

the SUBJECT PREMISES could lead to evidence of child exploitation offenses.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES³

37. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been

³ As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

38. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data

during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

39. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a

user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the SUBJECT PERSON's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of the SUBJECT PERSON's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

40. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. REQUEST FOR SEALING

41. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the

application and search warrant affidavit. I believe that sealing is necessary because the items and information to be seized is relevant to an ongoing investigation into criminal conduct involving minor victims and as far as I am aware, the target of this investigation remains unaware that he is being investigated. Disclosure of the search warrant affidavit at this time would seriously jeopardize the investigation, as such disclosure may provide an opportunity to destroy evidence, change patterns of behavior, or allow flight from prosecution. Further, based upon my training and experience, I have learned that online criminals often search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on this continuing investigation and may severely jeopardize its effectiveness.

IX. CONCLUSION

42. For all the reasons described above, there is probable cause to believe that AYALA has committed a violation of Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography and attempted possession of child pornography). There is also probable cause to believe that evidence, fruits, and instrumentalities of violations Title 18, United States Code, Sections 2251(a) (sexual exploitation of children and attempted sexual exploitation of children); Title 18, United States Code, Section 2252A(a)(2) (distribution and

receipt of child pornography and attempted distribution and receipt of child pornography); and Title 18, United States Code, Section 2252A(a) (5) (B) (possession of child pornography and attempted possession of child pornography) (collectively, the "Subject Offenses"), as described in Attachment B will be found in a search of the SUBJECT PREMISES and the SUBJECT PERSON described in Attachments A-1 and A-2.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 2nd day of April, 2025.

A handwritten signature in black ink, reading "Patricia Donahue". The signature is written in a cursive, flowing style. Below the signature is a horizontal line.

HONORABLE PATRICIA DONAHUE
UNITED STATES MAGISTRATE JUDGE

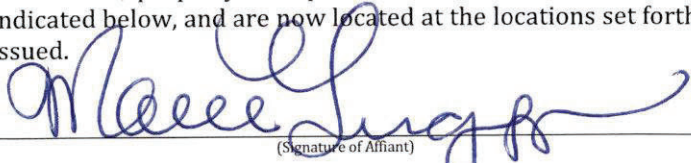
EXHIBIT 1

SW NO. _____

STATE of CALIFORNIA, COUNTY of LOS ANGELES,
SEARCH WARRANT and AFFIDAVIT
(AFFIDAVIT)

Detective Marine Gevorgyan, Serial No. 41253, swears under penalty of perjury that the facts expressed by him/her in the attached and incorporated **Affidavit** are true and that based therein he/she has probable cause to believe and does believe that the articles, property, and persons described below are lawfully seizable pursuant to Penal Code Section 1524 et seq., as indicated below, and are now located at the locations set forth below. Wherefore, Affiant requests that this Search Warrant be issued.

HOBBS SEALING REQUESTED: ☐ YES ☒ NONIGHT SEARCH REQUESTED: ☐ YES ☒ NO


 (Signature of Affiant)

(SEARCH WARRANT)

THE PEOPLE OF THE STATE OF CALIFORNIA TO ANY PEACE OFFICER IN THE COUNTY OF LOS ANGELES: proof by affidavit, having been this day submitted to me by Marine Gevorgyan that there is probable cause to believe that the property or person described herein may be found at the location(s) set forth herein and that it is lawfully seizable pursuant to Penal Code Section 1524 et seq., as indicated below by "☒"(s), in that:

- ☐ property was stolen or embezzled;
- ☐ property or things were used as the means of committing a felony;
- ☐ property or things are in the possession of any person with the intent to use them as a means of committing a public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their being discovered;
- ☐ property or things to be seized consist of any item or constitute any evidence that tends to show a felony has been committed, or tends to show that a particular person has committed a felony;
- ☒ property or things to be seized consist of evidence that tends to show that sexual exploitation of a child, in violation of Section 311.3, or possession of matter depicting sexual conduct of a person under the age of 18 years, in violation of Section 311.11, has occurred or is occurring;
- ☐ there is a warrant to arrest a person;
- ☐ a provider of electronic communication service or remote computing service has records or evidence, as specified in Section 1524.3, showing that property was stolen or embezzled constituting a misdemeanor, or that property or things are in the possession of any person with the intent to use them as a means of committing a misdemeanor public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery;
- ☐ property or things to be seized include an item or any evidence that tends to show a violation of Section 3700.5 of the Labor Code, or tends to show that a particular person has violated Section 3700.5 of the Labor Code;

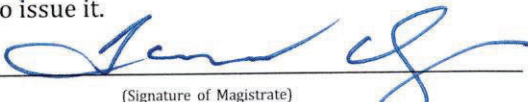
You are Therefore COMMANDED to SEARCH: (premises, vehicles, persons)

See Attached and Incorporated Description Page – Attachment A

For the FOLLOWING PROPERTY, THING(s), or PERSON(s):

See Attached and Incorporated Description Page – Attachment B

AND TO SEIZE IT / THEM IF FOUND and bring it / them forthwith before me, or this court, at the courthouse of this court. This **Search Warrant and Affidavit** and attached and incorporated **Affidavit** were sworn to as true and submitted to me on this day of 8/7, 2023, at 10:30 A.M. / P.M. Wherefore, I find probable cause for the issuance of this Search Warrant and do issue it.


 (Signature of Magistrate)

HOBBS SEALING APPROVED: ☐ YES ☒ NO
 NIGHT SEARCH APPROVED: ☐ YES ☒ NO

Judge of the Superior Court of California, County of Los Angeles, South District, Dept. 1

TOMSON T. CALA, JUDGE
 (Magistrate's Printed Name)



SW & A1

acc
31745

SEARCH WARRANT AND AFFIDAVIT

ATTACHMENT "A"

You are Therefore COMMANDED to Search:

THE INTERNET SERVICE PROVIDER known as Charter Communications, Inc.

Attn: Legal Response Operations Center

12405 Powerscourt Dr.

St. Louis, MO 63131

Phone: (314) 394-9702

Fax: (314) 909-0609

Email: leroc@charter.com

Service via fax or online submission: <https://clrp.spectrum.com>

THE INTERNET SERVICE PROVIDER known as: Google LLC

1600 Amphitheatre Parkway

Mountain View, CA. 94043

Attn: Custodian of Records

Phone: (844) 383-8524

Email: uslawenforcement@google.com

Service via digital upload: Law Enforcement Request System (LERS)

THE ONLINE SERVICE PROVIDER known as Snap Inc.

Attn: Custodian of Records

2772 Donald Douglas Loop

North Santa Monica, CA 90405

Service via upload to Snapchat Law Enforcement Service System: less.snapchat.com

31745

SEARCH WARRANT AND AFFIDAVIT

ATTACHMENT "B"

Spectrum

FOR THE FOLLOWING RECORDS:

Records from the above listed Service Provider for the IP Address: **142.129.44.180 on 07/25/2022 at 04:09:42 UTC**

In compliance with California Electronic Communications Privacy Act referenced by California Penal Code § 1546.1(d)(1), each of the types of records specified below associated with the Spectrum account shall be for the period of 07/20/2022 PDT to 08/07/2023 PDT. The provided records shall be reviewed for evidence related to the crime(s) of: 311.11 of the California Penal Code: Child Sexual Abuse Material (possession, manufacture, and distribution).

IP Address Logs: All information related to IP addresses used for the creation of the account as well as any IP address assigned to the Target Account.

Location Information: Any collected location information including but not limited to, latitude & longitude data, GPS coordinates, and known service address data associated with the Target Account's activity.

Subscriber Information: Subscriber information to include name, address, phone number, contact information, billing address, service address, email address, and phone numbers, payment information such as your payment card or bank account information; information related to a credit application for Spectrum Services, Social Security number, driver's license number or other government issued identifier, passwords, images, voice recordings, or other personal identifiers, additional accounts, custom settings or preferences, and dates associated with account creation and/or suspension for the above listed Target Account(s).

SEARCH WARRANT AND AFFIDAVIT

Google LLC**FOR THE FOLLOWING RECORDS:**

Records from the above listed Service Provider for the Email Address: **ayalahenry818@gmail.com**

In compliance with California Electronic Communications Privacy Act referenced by California Penal Code § 1546.1(d)(1), each of the types of records specified below associated with the Google LLC account shall be for the period of 07/20/2022 PDT to 08/07/2023 PDT. The provided records shall be reviewed for evidence related to the crime(s) of: 311.11 of the California Penal Code: Child Sexual Abuse Material (possession, manufacture, and distribution).

Device Information: Records of the device(s) used by the Target Account to access Google LLC services. The records shall include Device attributes including but not limited to operating system information, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins; Device operation information about operations and behaviors performed on the device such as whether a window is foregrounded or backgrounded, or mouse movements to help distinguish humans from bots; Unique identifiers, device IDs such as GAID or IDFA, and other identifiers from games, apps or accounts you use, and Family Device IDs, or other identifiers unique to Google Inc. products associated with the same device or account; Device signals including Bluetooth signals and MAC identifiers, and information about nearby Wi-Fi access points, beacons, and cell towers; Data from device settings such as access to GPS location, camera or photos; Network and connection information such as the name of the mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and information about other devices that are nearby or on the Target Account network; and Cookie data stored on the Target Account device, including cookie IDs and settings.

Google Files: Records of the Target Accounts use of the Google Files app to include the names of files deleted using the Google Files app, if available, and information about files that were synced to Google drive or shared via the app.

SEARCH WARRANT AND AFFIDAVIT

1 **IP Address Logs:** Information related to IP addresses used for the creation of the account whenever that
2 may have occurred as well as any IP address assigned to the Target Account during the time period
3 specified above.

4 **Subscriber Information:** Basic registration or customer information to include name, address, phone
5 number, contact information, additional accounts, and dates associated with account creation and/or
6 suspension for the above listed Target Account.

7 **Gmail Records:** Google Gmail records related to the Target Account to include subscriber registration
8 information; sign-in IP addresses and associated time stamps; email header information; and all Google
9 LLC stored electronic communications including saved, deleted, sent, stored, & draft email; stored notes;
10 stored chats and chat logs; account histories; attached files to include digital images, videos, documents,
11 links, and any other files associated with the Target Account.

12 **Google Pay:** Information contained in the associated Google Pay account including transactions,
13 purchases, money transfers, payment methods, including the full credit card number and/or bank account
14 numbers used for the transactions, and address book.

15 **Call Detail Records:** Records for the Target Account commonly known as Call Detail Records (CDR)
16 for the period described. Such records shall include Target Account inbound and outbound calls, sent
17 and received text messages with the associated text message content if available and, indications of calls
18 being sent to voicemail, and data connections with amount of data uploaded/downloaded. These records
19 shall also include associated cell-site records with sector, date, time, direction, and duration.

20 **Location Information:** Records of location-related information to include the Target Account's location,
21 frequently visited places, and the businesses and people the Target Account is near that Google LLC uses
22 to provide Google Products and ads. Location records shall include "precise device location", IP
23 addresses, and information from the Target Account use of Google Products such as check-ins. Location
24 information shall also include the identifiers and specific location (including address or GPS coordinates
25 and location name) of Bluetooth beacons and Wi-Fi access points that the Target Account's device
26 observed.

SEARCH WARRANT AND AFFIDAVIT

1 **Google Docs:** Stored Google Docs records to include Docs, Sheets, Slides, and Forms to include records
2 of collaboration and sharing that show who these file(s) were shared with or accessed by and shall
3 include archived copies of Docs, Sheets, Slides, and Forms.

4 **Google Drive:** Stored files in Google Drive stored by or accessible to the Target Account to include the
5 files EXIF or metadata and records that indicate if a file was shared or accessed by anyone other than the
6 listed Target Account with their associated account identifiers.

7 **Google Photos:** Stored photo and video files to include associated metadata & geo-location data and
8 associated album name, photo image tags provided by the Target Account, tagged photos and the
9 identities of persons tagged in the Target Account's photos if associated with a Google account.

10
11 **Snap Inc.**

12 FOR THE FOLLOWING RECORDS:

13 Records from the above listed Service Provider for the Account: **cocohennn**

14 In compliance with California Electronic Communications Privacy Act referenced by California Penal
15 Code § 1546.1(d)(1), each of the types of records specified below associated with the Snap Inc. account
16 shall be for the period of 07/20/2022 PDT to 08/07/2023 PDT. The provided records shall be reviewed
17 for evidence related to the crime(s) of: 311.11 of the California Penal Code: Child Sexual Abuse Material
18 (possession, manufacture, and distribution).

19
20 **Device Information:** Records of information collected about the devices the Target Account used to
21 access Snap Inc. services to include information about the hardware and software, operating system
22 version, device memory, advertising identifiers, unique application identifiers, apps installed, unique
23 device identifiers, browser type, language, battery level, and time zone, information from device sensors,
24 such as accelerometers, gyroscopes, compasses, microphones, headphone connection status; and
25 information about the Target Account's wireless and mobile network connections, such as mobile phone
26 number, service provider, and signal strength.

SEARCH WARRANT AND AFFIDAVIT

1 **Subscriber Information:** Subscriber Information to include username, password, email address, phone
2 number, date of birth, profile pictures, name, other useful identifying information, and commerce related
3 information such as debit or credit card number and its associated account information.

4 **Communication Content:** Records of communication with other Snapchatters, including the complete
5 message content, Snapchatter's names, the time and date of the communications, records of the Target
6 Account's interactions with messages such as opening a message or capturing a screenshot, bitmoji
7 reactions, and direct chat replies as well and records of communication with customer support. These
8 records shall also include Audio or Video calls using the Snapchat App and their associated records such
9 as dates and times of calls, call participants, duration of call, and stored call content if available.

10 **Location Information:** Records of precise location information associated with the Target Account
11 including GPS, wireless networks, cell towers, Wi-Fi access points, and other sensors, such as
12 gyroscopes, accelerometers, and compass data collected by Snap Inc.

13 **Camera and Photos:** Records of Snap Inc. collected or user uploaded images and videos and other
14 information from the Target Account device's camera and photos including associated exif or metadata.

15 **Content Information:** Records of content collected by Snap Inc. that the Target Account created, such
16 as custom stickers, scans, and information about the content the Target Account create or provide, such
17 as if the recipient has viewed the content and the metadata that is provided with the content.

18
19
20 **Authorization to implement special procedure(s):** The Affidavit filed herewith has demonstrated legal
21 justification for the implementation of the following special procedures which shall be employed by the
22 officers who execute this warrant:
23

24 California's Electronic Communications Privacy Act (ECPA) ORDER

25 IT IS HEREBY ORDERED that any information obtained through the execution of this warrant that is
26 unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or

SEARCH WARRANT AND AFFIDAVIT

disclosure absent an order from the Court, or to comply with California code 1054 and Brady v Maryland.

Authenticity of Record ORDER

IT IS HEREBY ORDERED that In compliance with the California Electronic Communications Privacy Act, the Service Provider listed in the search warrant shall provide a valid "Authenticity of Records" document consisting of an affidavit which meets requirements of California Evidence Code section 1561 and that the document be returned to the affiant along with a copy of the requested records.

California Penal Code Prohibited Violation Attestation

In compliance with the requirements outlined in California Penal Code § 1524.2(c) & § 1546.5(a) your affiant attests that the evidence sought in this search warrant is not related to an investigation into, or enforcement of, a prohibited violation, as defined in California Penal Code § 629.51.

Extension Date of Return to Search Warrant

IT IS HEREBY ORDERED, the affiant or representative of the Los Angeles Police Department need not return this warrant and produce the records within the required days of service to this court for good cause demonstrated in the affidavit. Instead, the warrant and records shall be produced promptly upon receipt. If the requested records are not provided to your affiant within 90 days of the execution of this search warrant, said affiant shall return a notice informing the court of the non-production of records or petition the Court for an extension on or before 11/05/2023.

Non-Disclosure ORDER

The affidavit herein has established sufficient reason to believe that immediate compliance with the notice requirements set forth in Penal Code § 1546.2(a) would result in otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Jo
Doc
3/17/25

SEARCH WARRANT AND AFFIDAVIT

1 IT IS HEREBY ORDERED that pursuant to Penal Code § 1546.2(b)(1), the Service Provider(s) listed in
2 the search warrant shall not notify the listed Target Account(s) of the existence of this search warrant
3 until the passage of 90 days from the date the warrant was executed.
4

5 Target Notification Delay ORDER

6 IT IS HEREBY ORDERED that, pursuant to the delayed notice provisions of Penal Code § 1546.2(b)(1),
7 notification to the target of the investigation shall be delayed for a period of 90 days. Upon expiration of
8 the period of delay of the notification, the Los Angeles Police Department shall submit to the California
9 Department of Justice within three days of the execution of the warrant a notice that includes information
10 about the target of the investigation, that said information has been compelled or obtained, and states
11 with reasonable specificity the nature of the government investigation under which the information is
12 sought. This notice will include a copy of all electronic information obtained or a summary of that
13 information and a statement of the grounds for the court's determination to grant a notification delay to
14 the target. This notice is being provided to the California Department of Justice as the target of the
15 investigations has not been identified.
16
17
18
19
20
21
22
23
24
25
26

SEARCH WARRANT AND AFFIDAVIT

Order to Send Information

Responsive data, if any, may be delivered by sending to:

Detective Marine Gevorgyan


501 W Ocean Blvd #7460, Long Beach, CA 90802

(562) 624-4027

41253@lapd.online

And, by using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A, or similar statute or code. Detective Marine Gevorgyan can be reached at office number (562) 624-4027, or email address 41253@lapd.online.

Dated: 8/7, 2023


Judge of the Los Angeles County Superior Court



SEARCH WARRANT AND AFFIDAVIT

STATEMENT OF EXPERTISE:

Your affiant, Detective Marine Gevorgyan Serial No. 41253, herein referred to as I, is employed as a full time sworn law enforcement officer for the Los Angeles Police Department (LAPD) for over 10 years. I have received training in preliminary and follow-up investigations of criminal acts at the Los Angeles Police Academy. I have received various LAPD in-service and California POST training including but not limited to Vice School, Human Trafficking School, Detective School, Undercover Operations Training and ICAC (Internet Crimes Against Children) Training. I have been trained by the National Center for Missing and Exploited Children regarding the investigation of Cybertip reports. I am familiar with numerous methods, websites and social media platforms commonly used by persons to search for, download, upload, and or distribute images and/or videos depicting the sexual exploitation and/or abuse of minors. I have authored approximately 100 search warrants related to the investigation of Human Trafficking/sexual exploitation. I have also received training in the Spotlight program that is a non-profit organization that assists law enforcement with investigations in the areas of Human Trafficking, Pimping, Pandering, Child Pornography, and on-line crimes against children. I have more than 7 years of experience and expertise in the area of Human Trafficking, Pimping, Pandering, Prostitution and other child sexual-exploitation types of crimes. I have conducted over 100 interviews with suspects, victims, and witness regarding criminal acts of violence.

Based upon your Affiant's knowledge, experience, and training in child exploitation and child sexual abuse material investigations, and the training and experience of other law enforcement officers whom I have had discussions, your Affiant knows there are certain characteristics common to individuals involved in the receipt, distribution, and collection of child sexual abuse material. Child sexual abuse material collectors may receive sexual gratification, stimulation, and satisfaction from contact with children or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses.

SEARCH WARRANT AND AFFIDAVIT

1 This satisfaction may come from viewing children in person, in photographs, other visual media, or from
2 literature describing such activity. Collectors of child sexual abuse material often collect sexually
3 explicit or suggestive materials in a variety of media including photographs, magazines, motion pictures,
4 videotapes, books, drawings or other visual media. Child sexual abuse material collectors not only use
5 these materials for their own sexual gratification, they have been known to use these materials to lower
6 the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to
7 demonstrate the desired sexual acts.

8
9 Child sexual abuse material collectors typically retain pictures, films, photographs, magazines,
10 correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years. Due
11 to its illegal nature, child sexual abuse material is a scarce resource that collectors are reluctant to delete
12 or destroy. As such, collectors of child sexual abuse material often maintain their collections in a digital
13 or electronic format in a safe, secure and private environment. These collections are often maintained for
14 several years and are kept close by, usually at the collector's residence, to enable the collector to view the
15 collection, which is valued highly.

16
17 Child sexual abuse material collectors also may correspond with and/or meet others to share information
18 and materials. Once a child sexual abuse material collector makes a connection with another, these
19 relationships are highly coveted. Child sexual abuse material collectors rarely destroy correspondence
20 from other child sexual abuse material distributors or collectors and will often conceal such
21 correspondence as they do their sexually explicit material. They will often maintain list of names,
22 addresses, email addresses, telephone numbers, and usernames of individuals with whom they have been
23 in contact and who share the same interest in child sexual abuse material.

24
25 Collectors of child sexual abuse material prefer not to be without their child sexual abuse material for any
26 prolonged time period. This behavior has been documented by law enforcement officers involved in the

SEARCH WARRANT AND AFFIDAVIT

1 investigation of child sexual abuse material throughout the world.

2
3 Based on the details of this investigation outlined in this affidavit, your Affiant believes that the person(s)
4 described in the attachment to this search warrant exhibits the common characteristic described above is
5 someone involved in the distribution, receipt, possession, or collection of child sexual abuse material.

6
7
8 Based upon your affiant's knowledge, experience, and training in child exploitation and child sexual
9 abuse material investigations, and the training and experience of other law enforcement officers with
10 whom I have had discussions, your affiant knows there are certain characteristics common to individuals
11 involved in the receipt, distribution, and collection of child sexual abuse material. Child sexual abuse
12 material collectors may receive sexual gratification, stimulation, and satisfaction from contact with
13 children or from fantasies they may have viewing children engaged in sexual activity or in sexually
14 suggestive poses.

15
16 This satisfaction may come from viewing children in person, in photographs, other visual media, or from
17 literature describing such activity. Collectors of child sexual abuse material often collect sexually explicit
18 or suggestive materials in a variety of media including photographs, magazines, motion pictures,
19 videotapes, books, drawings or other visual media. Child sexual abuse material collectors not only use
20 these materials for their own sexual arousal and gratification, they have been known to use these
21 materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child
22 partner, or to demonstrate the desired sexual acts.

23
24 Child sexual abuse material collectors typically retain pictures, films, photographs, negatives, magazines,
25 correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years. Due
26 to it's illegal nature, child sexual abuse material is a scarce resource that collectors are reluctant to delete

SEARCH WARRANT AND AFFIDAVIT

1 or destroy. As such, collectors of child sexual abuse material often maintain their collections in a digital
2 or electronic format in a safe, secure and private environment. These collections are often maintained
3 for several years and are kept close by, usually at the collector's residence, to enable the collector to view
4 the collection, which is valued highly.

5
6 Child sexual abuse material collectors also may correspond with and/or meet others to share information
7 and materials. Once a child sexual abuse material collector makes a connection with another, these
8 relationships are highly coveted. Child sexual abuse material collectors rarely destroy correspondence
9 from other child sexual abuse material distributors or collectors and will often conceal such
10 correspondence as they do their sexually explicit material. They will often maintain lists of names,
11 addresses and email addresses, and telephone numbers, and usernames of individuals with whom they
12 have been in contact and who share the same interests in child sexual abuse material.

13
14 Collectors of child sexual abuse material prefer not to be without their child sexual abuse material for any
15 prolonged time period. This behavior has been documented by law enforcement officers involved in the
16 investigation of child sexual abuse material throughout the world.

17
18 Based on the details of this investigation outlined in this affidavit, your affiant believes that the person(s)
19 described in the attachment to this search warrant exhibits the common characteristics described above of
20 someone involved in the distribution, receipt, possession or collection of child sexual abuse material.

21 22 23 **BACKGROUND AND EXPLANATION OF SPECTRUM**

24 Charter Communications, Inc., also known as Charter Spectrum or Spectrum, is a telecommunications
25 and mass media company based in Saint Louis, Missouri that offers internet, cable, and telephone
26 services to consumers and businesses under the branding of Spectrum. Charter Communications acquired

SEARCH WARRANT AND AFFIDAVIT

1 Time Warner Cable, Time Warner's internet division known as Road Runner, and its sister company
2 Bright House Networks.
3

4 BACKGROUND AND EXPLANATION OF GOOGLE

5 Google LLC is a globally recognized technology company that specializes in a broad range of internet-
6 related services and products. Among the products and services Google offers are online advertising
7 technologies, cloud computing, hardware and software products, search engine, and productivity
8 services. Google's core search engine is a widely popular product and offers users fast and accurate
9 search results. Other work and productivity services offered by Google include Google Docs, Google
10 Sheets, and Google Slides. The company also offers a cloud storage service, Google Drive, and an email
11 service, Gmail.
12

13 Google offers multiple communication services such as video chat, instant messaging, and voice
14 assistants, including Google Allo, Duo, Hangouts, and Google Assistant. The company also offers
15 mapping and navigation services such as Google Maps, Google Earth, Waze, Street View, and language
16 translation through Google Translate. Google has developed and leads the Android mobile operating
17 system and the Google Chrome web browser. Additionally, the company offers Internet Service Provider
18 and Mobile Telephony services such as Google Fiber, Google Fi, and Google Station.
19

20 Google collects user information in various ways, such as through user registration data and monitoring
21 user activity. Registration information may include name, gender, birthdate, and phone number. Google
22 tracks direct product usage, including recent Google searches, visited websites, and usage of smart home
23 devices. It also records accurate location information, videos watched, voice interactions with Google
24 Assistant, and voice recordings. Aggregated data is generated by combining search and viewing activity
25 to determine user preferences and interests. This data is used to create a digital profile of users that
26 Google primarily uses for targeted advertising and marketing data analytics.

SEARCH WARRANT AND AFFIDAVIT

BACKGROUND AND EXPLANATION OF THE SNAPCHAT APPLICATION

Snapchat is both a messaging platform and a social network that enables users to connect with their contacts using both a mobile app and a new browser based interface. Users can "chat" with their friends by sending them photos or short videos up to 10 seconds long, overlaying text on these photos and short videos, by sending plain text to another user, or by audio and video calls. One of the most unique things about Snapchat is the ephemeral components of the content that gets shared on it. Photos, videos, and unsaved text messages are automatically deleted a few seconds after they've been viewed by their recipients. Snapchat also provides a news feed feature where the user can post photos and videos that could be viewed by their friends as a story clip rather than as a private or group message. These clips, called "stories", are posted for 48 hours only before they are automatically deleted.

Before a user can use Snapchat they must create an account consisting of personally identifiable information and/or information that may provide additional investigative avenues for which additional search warrants or other legal process may be sought. The initial stage of creating an account is selection of a unique username. This name cannot be changed and remains as the identifiable account name for the profile. A new user can additionally create a 'vanity name' which is capable of being modified and can contain emojis, symbols or other characters that are not allowed for the account username. Both the username and vanity name are visible to other Snapchat users, however, users commonly reference the vanity name when identifying a Snapchatter. Vanity names and usernames can pose investigative challenges and initial confusion when researching Snapchat accounts. It is important to note that Snapchat does not have the technical capability to locate Snapchat accounts based upon vanity names. Snapchat users are immediately notified if the recipients of their Snapchat messages, also known as "snaps", try to take a screenshot of the snaps. Screenshots can indeed be captured if a user does it quickly and the sender is always notified about it right away. Despite this notification feature there exists several methods and apps that are capable to covertly saving snaps and bypassing this feature.

SEARCH WARRANT AND AFFIDAVIT

STATEMENT OF PROBABLE CAUSE:

On 07/26/2022, Snapchat submitted a report to the National Center for Missing and Exploited Children (NCMEC) regarding an incident of child sexual abuse material being possessed or transmitted using their service. The report was received by NCMEC staff on 07/26/2022. The report was subsequently assigned to the Los Angeles Police Department under CyberTip number 129293315. (See Exhibit A) The incident was ultimately assigned to your affiant for further investigation. This CyberTip is connected to (7) additional Cybertips No. 129140761, 164322023, 164322025, 164322029, 164322044, 164322047, and 164333436.

While NCMEC CyberTips contain many details of the users or persons involved in the incident, they often do not contain a complete explanation of exactly how child sexual abuse material was uploaded, downloaded, sent or received using the Snapchat service. As such, not every detail about the incident is known to your affiant. Your affiant does know that CyberTip number 129293315 contained user information for the person(s) involved as collected by Snapchat. The report stated that a person whose true identity has yet to be confirmed was using IP Address 142.129.44.180 and the following profile information:

Screen/User Name: cocohennn

Date of Birth: 03-22-1997

Email Address: ayalahenry818@gmail.com

IP Address: 142.129.44.180 on 07-25-2022 04:09:42 UTC

The CyberTip at issue, number 129293315, was submitted by Snapchat without an employee viewing the attached files as indicated within the PDF report. Your affiant knows that this CyberTip was originally submitted to the Los Angeles Police Department, however, your affiant was unable to determine if appropriate legal process has been secured authorize viewing the file(s) attached to the report. Your affiant or a member of the task force authored a search warrant to view the files submitted by Snapchat in

SEARCH WARRANT AND AFFIDAVIT

1 compliance with the requirements of U.S. v Wilson. Using this authorization, your affiant has viewed the
2 file(s) and provided written descriptions of the file(s) provided by Snapchat below:

3
4 **File Name:** cocohennn-None-c74b0964-8d69-44a9-9749-5b9aab6ea1a6~81-88a5d47234.mp4

5 **File Hash:** 65eaa119cdd6631d65c8ee6da7a2144d

6 **File Description:** Video is approximately 20 seconds long depicting a male adult laying down with his
7 erect penis inside child. Male is having anal intercourse with a female child who is positioned on top of
8 him with her back towards him. Child underwear is moved to the left side of her buttocks as they engage
9 in anal intercourse. The child appears to be approx. 10-12 years of age.

10
11 Snapchat also recorded the IP address related to this incident of 142.129.44.180. This IP address has
12 been determined to be serviced by Spectrum with service to an unknown person in the Pacoima CA area.
13 Your affiant knows that Spectrum will have Subscriber Information records that will help to positively
14 identity the person(s) involved in this incident. Your affiant requests that the court authorize a search
15 warrant for the records outlined in Attachment B that may constitute potential evidence as well as records
16 that may lead to determining the true identity of the person(s) responsible for this possession,
17 distribution, or manufacture of child sexual abuse material.

18
19 Your affiant knows that Google LLC maintains records related to the mobile phones and digital devices
20 used to access their services as their normal course of business. These device attributes such as IMEI
21 uniquely identify individual devices and can be valuable in criminal investigations as they uniquely
22 identify mobile devices on cellular networks.

23
24 Your affiant knows that Google Files is an Android app created by Google that helps users file and
25 manage files stored on the user's phone. The app is frequently used to delete old or unnecessary files on
26 the phone or can be used to offload stored files to Google Drive and free up local storage. Google Files

SEARCH WARRANT AND AFFIDAVIT

1 can also share locally stored files through near-field communication, bluetooth, messaging, and
2 connected services like Google Duo or Hangouts.

3
4 Your affiant knows that an Internet Protocol (IP) address is a numerical label assigned to devices
5 communicating on the Internet and that the Internet Assigned Numbers Authority (IANA) manages the
6 IP address space allocations globally. An IP address enables the methods of communication between
7 devices on the Internet; it is a number that uniquely identifies a device on a computer network and, using
8 transport protocols, moves information on the Internet. Every device directly connected to the Internet
9 must have a unique IP address. Simply put, an IP address is similar to the address on your house. To
10 mail a letter to a person, you must know that address where the letter is to be sent. In order to receive a
11 response, the envelope must contain the original senders address so that the recipient knows where to
12 respond.

13 An IP address is typically comprised of four series of numbers separated by periods and is most
14 commonly represented as a 32-bit number such as 54.71.229.212, known as an Internet Protocol Version
15 4 (IPv4). A newer version, IPv6, is swiftly becoming the standard and is represented as a 128-bit number
16 such as 2001:db8:0:1234:0:567:8:1.

17 In most instances, consumers purchase internet service through an Internet Service Provider ("ISP"). The
18 ISP then provides IP addresses to the consumer. IP addresses are owned by the Internet Service Provider
19 and leased to a subscriber/customer for a period of time. They are public and visible to others as you surf
20 the Internet. The lessee has no expectation of privacy due to the public nature of IP addresses. There are
21 many publicly available websites that allow anyone to look-up the owner of an IP address. The IP
22 address contain information on the geographic location of the connection. There are two different types
23 of Internet Protocol addresses. The first is a dynamic IP address, which means the user's IP address may
24 change each time they log on to the Internet. The frequency in which this address changes is generally
25 controlled by the Internet Service Provider and not the user. The other type of IP address is a static IP
26 address, which means that a user is assigned a specific IP address that remains constant every time they

So
ac
3/24/25

SEARCH WARRANT AND AFFIDAVIT

1 log on to the Internet. Static IP addresses are traditionally used commercially and are expensive, making
2 them rarely seen in residential accounts.

3 There are services that allow individuals obscure the IP address issued by their ISP, called Virtual Private
4 Networks ("VPNs"). An individual who uses a VPN routes their internet traffic through the VPNs IP
5 address so the publicly available IP address points to the VPN and not the consumer's actual ISP. VPNs
6 allow individuals to make it look like they are connecting to the internet from anywhere in the world.

7 As it relates to this case and investigation, I know that media platforms such as Google maintain and log
8 of IP addresses. This data is obtained when a user accesses their account or logs into their account. Your
9 affiant believes that obtaining IP address information from Google on the suspect account as it relates to
10 this investigation will help investigators locate the suspect.

11
12 I know from my training and experience that those who subscribe to internet service providers and
13 electronic service providers, often provide personal information that may be used in the identification of a
14 person's account, identity, location, service information, and dates related to said service. Such
15 information may contain, but not limited to: social security numbers, names, addresses, dates of birth,
16 phone numbers, account holder information, service transfer information, place of employment. Said
17 information may also contain a list of those who are authorized to make changes to said accounts.

18
19 Your affiant knows that persons involved in the possession and distribution of Child Sexual Abuse
20 Material (CSAM) often do not create usernames that would tend to identify themselves. However,
21 communications platforms and websites that trade CSAM often require registration and users will sign up
22 with email addresses. Believing that the emails are not public, suspects often use real email addresses
23 that they use elsewhere on the internet. Sometimes a review of the email stored within the account can be
24 the only information that identifies the subject responsible for trading CSAM. For example, if that email
25 address was listed for an unrelated online purchase, they may receive a receipt with their true name and
26 shipping address. An analysis of the stored email is requested to provide contextual clues as to who is

SEARCH WARRANT AND AFFIDAVIT

1 responsible for the account.

2
3 Google maintains a unified payment service, which combined Google Wallet and Android Pay into one
4 service. Google Pay is an application that stores purchase and payment activity, along with individual
5 credit card, debit card, and gift card information associated with the Google subscriber(s). Google Pay
6 allows subscribers to send and receive money from a mobile device or computer at no cost to either the
7 sender or receiver and facilitates e-purchases. I believe this the data contains information relevant to this
8 investigation including records of purchases and payments, as well as money transfers and
9 communications with unknown co-conspirators and/or witnesses, and other information concerning the
10 ongoing investigation

11
12 Your affiant knows that telecommunication providers retain call detail records related to customer's
13 mobile phone usage as a normal course of business. These records are useful for investigators as they
14 tend to show what persons and businesses that the target of the investigation communicates with and the
15 frequency of the communication. The dates, times, and recipient of text messages, both Simple Message
16 Service (SMS) and Multimedia Messaging Service (MMS) are recorded by telecommunication providers
17 thought the content of messages is not commonly retained. Your affiant knows that in investigations
18 involving child sexual abuse material, call detail records are most closely related to incidents where illicit
19 images and videos are being sent to or solicited from minors. Call Detail Records will provide records
20 that may help to prove a connection between the suspect and victim and provide evidence that a
21 multimedia message was sent. Your affiant believes that these records would be useful in this
22 investigation and requests that they be provided by Google LLC.

23
24 Your affiant has been told that Google collects and retains location data from devices; The most common
25 source of location data is derived from devices using the Android operating system, however it can be
26 collected from Apple devices as well. Google uses this information for location-based advertising,

SEARCH WARRANT AND AFFIDAVIT

1 location-based search results, navigation, and for use and integration with third-party applications and
2 services. According to documentation from Google, information from security researchers, media reports,
3 and other law enforcement sources, this information is derived from several different technologies built
4 into smartphones and other mobile devices. These location technologies include: Global Position System
5 (GPS) data, cell site/cell tower information derived from signal strength measurement and signal
6 multilateration, sometimes referred to as triangulation, Wi-Fi signal strength measurement, and signal
7 multilateration, Bluetooth readings from nearby beacons and other mobile devices with the technology
8 activated, and data derived from sensors embedded in the mobile device such as accelerometer,
9 barometer, gravity sensor, magnetic field sensor, orientation sensor, and/or proximity sensor. The
10 combination of these technologies can provide law enforcement investigators with historical location data
11 more precise than those available from traditional sources of information such as cell site location
12 information from the cellular carrier. While the specific parameters of when this location data is collected
13 are not entirely clear, it appears that Google collects or refreshes this data whenever one of their services
14 is activated and/or whenever there is an event on the mobile device such as a phone call, text messages,
15 internet access, specific application activation, email access or updates to an email account, and system
16 updates.

17
18 Your affiant knows through training and investigative experience that Google offers their users access to
19 free, web-based alternatives to existing word processing, spreadsheet, and presentation software. The
20 documents created by their software are stored in the user's account and are accessible from any device or
21 platform as long as the user knows the password. These documents can include those created by the user,
22 modified or edited by the user, or shared with the user by others. Your affiant believes this information
23 may contain information in the form of notes, files, and spreadsheets relevant to this investigation.

24
25 Your affiant knows that persons who collect child sexual abuse material typically save their images and
26 videos to Google Drive as a way to keep the material accessible, but off of their computer or mobile

SEARCH WARRANT AND AFFIDAVIT

1 phone. Your affiant believes that Google Drive records will help your affiant you to positively identify
2 the target and to possibly obtain additional evidence.
3

4 Your affiant is seeking to search within the Google Photos section of the suspect account. Your affiant
5 knows that images saved to devices linked to Google accounts will most often save to the Google Photos
6 storage. Your affiant believes it is probable that there will be evidence related to this crime such as Child
7 Sexual Abuse Material stored within that account. Your affiant knows that this is a common place that
8 persons involved in Child Sexual Abuse Material will store images and videos. Additionally, it is likely
9 that there will be evidence of ownership stored within that account such as photos or selfies of the
10 suspect.
11

12 Your affiant knows based on personal knowledge, training and investigative experience that Snapchat
13 account information often list the make and model of the mobile phones or internet browser type used by
14 the Target Account to access Snapchat services. This information will assist investigators in determining
15 what type of phone belonged to the suspect at the time of the crime. This would further assist in the
16 recovery of the device and ultimately assist in further collection of digital evidence through that phone
17 that would support the investigation.
18

19 Your affiant has been told that Snapchat is designed with privacy in mind and most messages are sent by
20 overlaying text on top of photos or videos that delete themselves in 10 seconds or less. Your affiant has
21 also been told that Snapchat users can send messages to each other in a more traditional text messaging
22 style conversation and these messages do not auto-delete. The context of these messages can be critical
23 in many aspects of this investigation either as direct evidence of the crime or contextually by helping to
24 identify parties participating in conversations.

25 In Child Sexual Abuse Material investigations (CSAM), it is common for CSAM to be sent from one
26 user to another in a self-deleting fashion. However, plain text responses to the sent photos or video may

SEARCH WARRANT AND AFFIDAVIT

1 give your affiant an understanding of what the content of the media was.

2
3 Your affiant knows based upon knowledge, training and investigative experience that reviewing a
4 Snapchat accounts location information would greatly assist in determining the suspects location prior to,
5 during and after the crime. Your affiant has been told that the Snapchat app records a users location and
6 send that information back to Snap Inc. while the app is being used and sometimes when the app is
7 simply active in the background of the user's phone. Your affiant knows that Snapchat poses a
8 significant investigative challenge in that the vast majority of accounts are not made with truthful or
9 accurate information and determining the identity of a Snapchat user can be difficult, especially in child
10 sexual abuse material investigations. By determining the locations collected by the Snapchat app, these
11 data points may provide valuable clues as to locations frequented by the user, possibly even their home
12 address. These data points may very well lead to a positive identification of the person responsible for
13 the account.

14
15 Your affiant knows based on knowledge, training and investigative experience that reviewing the photos
16 stored within a Snapchat account can assist in confirming the account belongs to the suspect. Your affiant
17 also knows that people in general will take pictures with friends and family and post these photos in their
18 Snap Stories. Photos like these, if present, are valuable evidence to establish connections between a
19 suspect and ownership of a Snapchat account.

20
21 Based on your affiants training and investigative experience, your affiant knows that suspects engaged in
22 criminal activity often use social media applications to communicate with victims and other accomplices.
23 Snapchat is a preferred communication method as messages are designed to delete themselves within 10
24 seconds of being viewed. Content from these social media platforms can contain evidence such as
25 photographs, videos, messages, and other forms of communication that helps investigators determine the
26 facts of the case.

80
one
3/24/25

SEARCH WARRANT AND AFFIDAVIT

1 Therefore, your affiant believes the Google, Spectrum and Snapchat accounts are in violation of
2 California Penal Code 311.11(a) – Possession of Child Pornography and 311.1(a) PC – Distribution
3 of Child Pornography. The requested content will not only further corroborate the suspects
4 activities as they relate to the possession and distribution of Child Pornography, but also identify
5 co-conspirators who the Google user may be associated with and obtaining, and/or trading Child
6 Pornography with. I believe sufficient probable cause exists for the issuance of the search warrant
7 to obtain the records described in attachment B.

8
9 Based on the information contained in this affidavit, including the description of the image described
10 above that depicts a minor child engaged in a sexual act with an adult, your affiant believes that sufficient
11 probable cause exists for the issuance of a search warrant to obtain subscriber information related to the
12 Charter Communications / Spectrum account associated with IP Addresses reported by Snapchat:
13 **142.129.44.180 on 07/25/2022 at 04:09:42 UTC** in violation of California Penal Code 311.11(a) –
14 Possession of Child Pornography.

16 Request For Warrant Return Extension Order

17 Your affiant knows through prior experience with Internet Service Providers, conversations with other
18 law enforcement officers, and previous law enforcement training that these companies often cannot
19 promptly comply with search warrants for a variety of reasons. Though the records sought in this
20 warrant are generally stored digitally, access to those records is restricted to a few representatives and
21 only upon the order of their legal department's approval. These issues are further compounded by the
22 volume of requests that Internet Service Providers receive from law enforcement agencies across the
23 country, and in some instances, law enforcement agencies from across the world. Furthermore, your
24 affiant knows that Internet Service Providers hold an extremely high number of records and that it can be
25 common to receive hundreds of pages of documents, if printed, in response to a search warrant. For these
26 reasons, your affiant believes that it is unlikely they will receive the requested records within the time

50
MC
3/24/25

SEARCH WARRANT AND AFFIDAVIT

1 required to return the warrant and records to this Court. Your affiant therefore requests this Court issue
2 an extension of up to 90 days to return the warrant and records aligning with the expiration of the Non-
3 Disclosure Order. However, your affiant assures the Court that the warrant and records will be returned
4 promptly upon their receipt. In the event that the requested records are not provided to your affiant
5 within 90 days of the execution of this search warrant, your affiant shall return a notice informing the
6 Court of the Internet Service Providers failure to produce records and may choose to petition for an
7 extension on or before 11/05/2023.

10 **Order to Seal Non-Evidentiary Information**

11 As required by privacy act provisions, items that are within the scope of this warrant will be copied and
12 retained by investigative agency. Investigating agents will then seal any information from the device that
13 is unrelated to the objective of the warrant and will not further review the information pending an order
14 from the Court.

17 **Request for Authenticity of Record Order**

18 In compliance with privacy act provisions, your affiant requests that the Service Provider listed in the
19 search warrant provide a valid "Authenticity of Records" document consisting of an affidavit which
20 meets requirements of California Evidence Code section 1561 and that the document be returned to the
21 affiant along with a copy of the requested records.

24 **Request for Non-Disclosure and Target Notification Delay**

25 It is requested that pursuant to the preclusion of notice provisions of Penal Code §1546.2(b)(1), the
26 Service Provider be ordered not to notify any person (including the subscriber, customer or owner of the

SEARCH WARRANT AND AFFIDAVIT

1 electronic communication or device information to which the materials relate) of the existence of this
2 warrant for 90 days. Upon expiration of the period of delay of the notification, if the target of the
3 investigations is still unknown, the government entity shall submit to the California Department of
4 Justice a notice that includes information about the target of the investigation, that said information has
5 been compelled or obtained, and states with reasonable specificity the nature of the government
6 investigation under which the information is sought. This notice will include a copy of all electronic
7 information obtained or a summary of that information and a statement of the grounds for the court's
8 determination to grant a notification delay to the target. If the target of the investigation has been
9 identified during this period, a notice shall be served upon, or delivered to by registered or first-class
10 mail, electronic mail, or other means reasonably calculated to be effective as specified by the court
11 issuing the order authorizing delayed notification, the identified targets of the warrant. This notice shall
12 be a document that informs the recipient that information about the recipient has been compelled or
13 obtained, and states with reasonable specificity the nature of the government investigation under which
14 the information is sought, includes a copy of the warrant, a copy of all electronic information obtained or
15 a summary of that information reflecting the number and types of records disclosed, the date and time
16 when the earliest and latest records were created, and a statement of the grounds for the court's
17 determination to grant a delay in notifying the individual. Your affiant believes that notification by the
18 Service Provider would result in otherwise seriously jeopardizing an investigation or unduly delaying a
19 trial.

20
21
22 Your affiant is aware that companies often have a policy of notifying their customers shortly after receipt
23 of process such as a search warrant. Your affiant believes notification to the suspect of receipt of this
24 Search Warrant would cause them to become aware of the law enforcement investigation which may
25 cause them to conceal, secrete, delete, destroy or encrypt the very evidence this affidavit for search
26 warrant seeks to retrieve and preserve. Your affiant also believes the suspect may attempt to dissuade

SEARCH WARRANT AND AFFIDAVIT

1 witnesses from cooperating with the law enforcement investigation and/or testifying in court. Notification
2 would also allow the suspect to conspire with others to create alibis and fabricate a version of events to
3 avoid successful prosecution. Each of these actions would seriously jeopardize the investigation and may
4 lead to an undue delay of the prosecution. Therefore, your affiant requests the company(s) identified in
5 the search warrant be prevented from disclosing the existence of the Search Warrant to the suspect or any
6 other person not directly involved with complying pending until further order of the Court.
7

8 I have reasonable cause to believe that grounds for the issuance of a search warrant exist, as set
9 forth in Section 1524 of the Penal Code of the State of California, based upon the aforementioned
10 information, facts and circumstances. I therefore request that the court issue a warrant authorizing a
11 search of the premises described in the Attachment(A) for the items listed in the Attachment(B).
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

Jo
me
3/24/25